ECS Configuration Change Request

Page 1 of Page(s)

1. Originator	2. Log Date:	3. CCR #:	4. Rev:	5. Tel:	6. Rm #:	7. Dept.
Henry Baez	8 SEP 00	00-0910	—	301-925-1025	2101D	SED

8. CCR Title: Install and test SGI patch to fix telnetd daemon security bug on IRIX 6.2 and 6.5 machines in IDG Test Cell.

9. Originator Signature/Date 9-8-2000	10. Class IN	11. Type: CCR	12. Need Date: 9/15/2000

13. Office Manager Signature/Date Jim Mather 9/8/00	14. Category of Change: Initial ECS Baseline Doc.	15. Priority: (If "Emergency" fill in Block 28). Routine

16. Documentation/Drawings Impacted:	17. Schedule Impact:	18. CI(s) Affected:

19. Release Affected by this Change: 5A	20. Date due to Customer:	21. Estimated Cost: None - Under 100K

22. Source Reference: ☒NCR (attach) □Action Item □Tech Ref. □GSFC □Other:
ECSed28075

23. Problem: (use additional Sheets if necessary)
SGI reported that exploitable buffer overflow has been discovered in telnetd daemon which can lead to root compromise. A local user account on the venerable systems is not required in order to exploit this telnetd daemon bug. The telnetd daemon can be exploited remotely over an un-trusted network.

Attach are the SGI Security Advisory and patch release notes

24. Proposed Solution: (use additional sheets if necessary)
SGI has released a patch for IRIX 6.2 and 6.5.X to fix this exploitable buffer overflow bug. The patches would be install in an appropriate version IDG Test Cell SGI machine to test affects of patches on the SGI machines. SGI patch 4050 on IRIX 6.2 IDG Test Cell SGI machines drpepper and protog1. SGI patch 4044 on IRIX 6.5 IDG Test Cell SGI machines camaro and protog2.

PATCH4044.TAR CHECKSUM - 18827 40 PATCH4050.TAR CHECKSUM - 39097 1160

25. Alternate Solution: (use additional sheets if necessary)
The telnetd daemon can be turned off which will prevent the exploit. This however might impact on maintenance, as it will require logging in on console.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)
Any SGI machine that can be access from outside ECS space can be exploited and compromise with very harmful results. One SGI machine that is root compromise would then open all the other machines to attacks. Production could be impacted severely.

27. Justification for Emergency (If Block 15 is "Emergency"):

28. Site(s) Affected: □EDF □PVC □VATC □EDC □ GSFC □LaRC □NSIDC □SMC □AK □JPL □EOC ☒ IDG Test Cell □Other

29. Board Comments:	30. Work Assigned To:	31. CCR Closed Date:

32. EDF/SCDV CCB Chair (Sign/Date): 9/11/00	Disposition: [✓ Approved] App/Com. Disapproved Withdraw Fwd/ESDIS ERB
33. M&O CCB Chair (Sign/Date):	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
34. ECS CCB Chair (Sign/Date):	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB

ORIGINAL